

What is claimed is:

1           1. A method of initiating performance of a computation on at least one untrusted  
2 computer, the method comprising:

3           partitioning the computation into a plurality of computational units that are  
4 combinable to generate a result for the computation;

5           generating at least one distractive computational unit;

6           initiating execution of both the at least one distractive computational unit and  
7 at least one of the plurality of computational units on the untrusted computer to  
8 inhibit reconstitution of the computation by an untrusted party.

1           2. The method of claim 1, wherein the distractive computational unit comprises a  
2 computational unit generated from partitioning a second computation.

1           3. The method of claim 2, wherein initiating execution of both the at least one  
2 distractive computational unit and at least one of the plurality of computational units  
3 includes interleaving the at least one distractive computational unit among multiple  
4 computational units from the plurality of computational units.

1           4. The method of claim 2, wherein partitioning the computation uses a different  
2 algorithm than that used to partition the second computation.

1           5. The method of claim 1, wherein the distractive computational unit comprises a  
2 dummy computational unit.

1           6. The method of claim 1, wherein the distractive computational unit comprises a  
2 computational unit generated from a second partitioning of the computation.

1           7. The method of claim 1, further comprising initiating execution of at least one  
2 of the plurality of computational units on a second computer.

1           8. The method of claim 1, further comprising initiating execution of all of the  
2 plurality of computational units on the untrusted computer.

1           9. The method of claim 1, wherein partitioning the computation into the plurality  
2 of computational units comprises partitioning using the Chinese Remainder Theorem  
3 (CRT).

1           10. The method of claim 9, wherein the computation includes a plurality of  
2 arguments, and wherein partitioning the computation into the plurality of computational  
3 units comprises:  
4           selecting a plurality of relatively prime moduli; and  
5           generating each computational unit by performing a modulo operation on each  
6 of the plurality of arguments using one of the plurality of relatively prime moduli.

1           11. The method of claim 10, wherein selecting the plurality of relatively prime  
2 moduli includes selecting each modulus from a superset of relatively prime moduli, the  
3 method further comprising:  
4           partitioning a plurality of computations into multiple computational units  
5 using different sets of moduli selected from the superset of relatively prime  
6 moduli; and  
7           initiating execution of computational units from multiple computations on the  
8 untrusted computer.

1           12. The method of claim 1, further comprising:  
2           receiving result data generated during execution of each of the plurality of  
3 computational units; and  
4           generating a result for the computation from the result data.

1           13. The method of claim 1, wherein the untrusted computer is coupled to a grid  
2           computing network.

1           14. The method of claim 13, wherein partitioning the computation is performed  
2           by a client computer coupled to the grid computing network.

1           15. The method of claim 13, wherein partitioning the computation is performed by  
2           a broker computer coupled to the grid computing network, the method further comprising  
3           receiving the computation from a client computer.

1           16. The method of claim 1, wherein partitioning the computation, generating the  
2           distractive computational unit, and initiating execution of both the distractive  
3           computational unit and the one of the plurality of computational units on the untrusted  
4           computer are performed by at least one computer coupled to the untrusted computer, the  
5           method further comprising communicating the distractive computational unit and the one  
6           of the plurality of computational units to the untrusted computer.

1           17. An apparatus, comprising:

2                 at least one processor; and

3                 program code configured to be executed by the at least one processor to  
4           initiate performance of a computation on at least one untrusted computer by  
5           partitioning the computation into a plurality of computational units that are  
6           combinable to generate a result for the computation, generating at least one  
7           distractive computational unit, and initiating execution of both the at least one  
8           distractive computational unit and at least one of the plurality of computational  
9           units on the untrusted computer to inhibit reconstitution of the computation by an  
10          untrusted party.

1           18. The apparatus of claim 17, wherein the distractive computational unit

2          comprises a computational unit generated from partitioning a second computation.

1           19. The apparatus of claim 18, wherein the program code is configured to initiate

2          execution of both the at least one distractive computational unit and at least one of the  
3          plurality of computational units by interleaving the at least one distractive computational  
4          unit among multiple computational units from the plurality of computational units.

1           20. The apparatus of claim 18, wherein the program code is configured to

2          partition the computation using a different algorithm than that used to partition the second  
3          computation.

1           21. The apparatus of claim 17, wherein the distractive computational unit

2          comprises a dummy computational unit.

1           22. The apparatus of claim 17, wherein the distractive computational unit

2          comprises a computational unit generated from a second partitioning of the computation.

1           23. The apparatus of claim 17, wherein the program code is further configured to  
2 initiate execution of at least one of the plurality of computational units on a second  
3 computer.

1           24. The apparatus of claim 17, wherein the program code is further configured to  
2 initiate execution of all of the plurality of computational units on the untrusted computer.

1           25. The apparatus of claim 17, wherein the program code is configured to  
2 partition the computation into the plurality of computational units using the Chinese  
3 Remainder Theorem (CRT).

1           26. The apparatus of claim 25, wherein the computation includes a plurality of  
2 arguments, and wherein the program code is configured to partition the computation into  
3 the plurality of computational units by selecting a plurality of relatively prime moduli,  
4 and generating each computational unit by performing a modulo operation on each of the  
5 plurality of arguments using one of the plurality of relatively prime moduli.

1           27. The apparatus of claim 26, wherein the program code is configured to select  
2 the plurality of relatively prime moduli from a superset of relatively prime moduli,  
3 wherein the program code is further configured to partition a plurality of computations  
4 into multiple computational units using different sets of moduli selected from the superset  
5 of relatively prime moduli, and initiate execution of computational units from multiple  
6 computations on the untrusted computer.

1           28. The apparatus of claim 17, wherein the program code is further configured to  
2 receive result data generated during execution of each of the plurality of computational  
3 units, and generate a result for the computation from the result data.

1           29. The apparatus of claim 17, wherein the untrusted computer is coupled to a  
2           grid computing network.

1           30. The apparatus of claim 29, further comprising a client computer coupled to  
2           the grid computing network and upon which the program code resides.

1           31. The apparatus of claim 29, further comprising a client computer coupled to the  
2           grid computing network and upon which the program code resides, wherein the program  
3           code is further configured to receive the computation from a client computer.

1           32. The apparatus of claim 17, wherein the program code resides on a separate  
2           computer coupled to the untrusted computer, and wherein the program code is further  
3           configured to communicate the distractive computational unit and the one of the plurality  
4           of computational units to the untrusted computer.

1           33. A program product, comprising:

2                   program code configured to initiate performance of a computation on at  
3           least one untrusted computer by partitioning the computation into a plurality of  
4           computational units that are combinable to generate a result for the computation,  
5           generating at least one distractive computational unit, and initiating execution of  
6           both the at least one distractive computational unit and at least one of the plurality  
7           of computational units on the untrusted computer to inhibit reconstitution of the  
8           computation by an untrusted party; and  
9                   a computer readable signal bearing medium bearing the program code.

1           34. The program product of claim 33, wherein the signal bearing medium  
2           includes at least one of a recordable medium and a transmission medium.